ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 36, Number 6, 2006

QUADRATIC RESIDUES OF CERTAIN TYPES

ALEXANDRU GICA

ABSTRACT. The main purpose of the paper is to show that if p is a prime different from $2, 3, 5, 7, 13, 37$, then there exists a prime number q smaller than p, $q \equiv 1 \pmod 4$, which is a quadratic residue modulo p. Also, it is shown that if p is a prime number which is not $2, 3, 5, 7, 17$, then there exists a prime number $q \equiv 3 \pmod 4$, $q < p$, which is a quadratic residue modulo p.

1. Introduction. In [**2**] it is shown that any $n \in \mathbf{N}$, $n > 3$, could be written as

$$n = a + b,$$

a, b being positive integers such that $\Omega(ab)$ is an even number. If $m \in \mathbf{N}$, $m \geq 2$, has the standard decomposition $m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$ then the *length* of m is $\Omega(m) = \sum_{i=1}^{n} a_i$. We put $\Omega(1) = 0$. In connection with the above quoted result, the following open problem naturally arises.

Open problem. *What numbers n can be written as $n = a^2 + b$, where a, b are positive integers, the length of b being an even number?*

Trying to solve this problem was the starting point for the main result of this paper.

Theorem 1. *Let p be a prime number $p \neq 2, 3, 5, 7, 13, 37$. There exists a prime number q such that $q < p$, $q \equiv 1 \pmod 4$ and $(q/p) = 1$.*

We will prove also a similar result which has, however, an elementary proof:

2000 AMS *Mathematics Subject Classification.* Primary 11A15, 11E25, 11R29.
Key words and phrases. Quadratic residue, length, numerus idoneus.
Received by the editors on March 22, 2004, and in revised form on April 9, 2004.